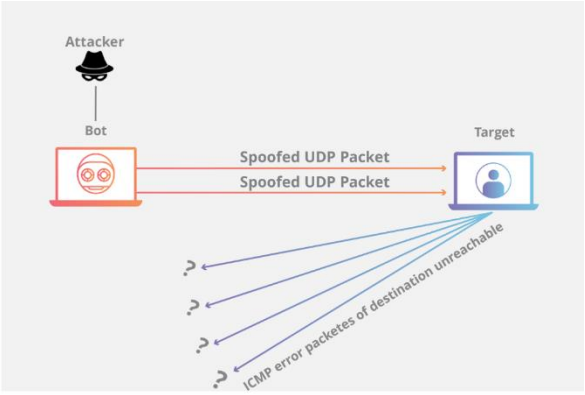
DDos UDP flood 防禦方式

107520504 歐亭昀、 107502518 王昱承、109522009 蕭盛澤

目錄：

一、 介紹

1. UDP flood 攻擊方式



DDos 攻擊：短時間內多個計算機(僵屍網路)對一個或多個目標伺服器產生大量請求，使伺服器鏈路擁塞或忙於處理攻擊請求，導致服務暫時中斷或停止，導致其正常使用者無法訪問。

UDP flood：大量 UDP 小包衝擊 DNS 伺服器或 Radius 認證伺服器、流媒體視頻伺服器。UDP flood 攻擊中，攻擊者可傳送大量偽造源 IP 位址的小 UDP 包。導致目標伺服器在理 UDP 封包並傳送大量回覆封包(回復無法送達 ICMP)時造成阻塞(造成此 ICMP 封包充斥著整個網路且影響網路頻寬)。也造成受攻擊者一直處於尋找可處理 UDP 封包應用程式及回傳 ICMP 給錯誤的來源端的忙碌狀態，被攻擊者的網路資源、系統內存、處理器資源也因此耗盡，進而影響到一般使用者正常存取該系統。

2. 何謂 TCP&UDP

TCP(Transmission Control Protocol)：

是一種雙向的通訊協定，特色是在接收端收到封包以後會回送一個「確認」的信，即需要“Three way handshake ”來建立虛擬連線，其優點是確保資料正確傳輸，以及可靠性。

UDP(User Datagram Protocol):

是一種單向的通訊協定，特色是想發封包時就直接丟，且不會對資料封包進行拆分與拼接。再來 UDP 具有單播、多播以及廣播的功能，但是並不具可靠性。而且 UDP 並沒有「壅塞控制」，只會以一恆定速率不斷丟封包，較容易掉封包。不過 UDP 也因為傳輸較快故比較適合時效性要求高且不再乎掉包的應用，例如:影像媒體，電話會議…等。

3. 殭屍網路介紹

殭屍網路(Zombie network)，即 BotNet 病毒的俗稱，病毒通常會隨著 e-mail、通訊軟體、電腦系統漏洞侵入電腦，再找一個程式做為之後發動攻擊的地方，並在之後執行到此被感染的程式時，電腦會遭到惡意執行者的控制。目前已知的用戶端/伺服器網路模型有星型網路拓樸、多個伺服器網路拓樸以及階層式網路拓樸。在任何模型中每一個魁儡程式都會連線到 Web 網域或 IRC 通道等命令中心資源，以便接收指示。透過使用集中式存放庫來為殭屍網路提供新命令，攻擊者僅需修改每個殭屍網路從命令中心消耗的來源資料，即可更新受感染機器的指示。

4. 使用工具介紹

目前現存有三套殭屍網路的基礎程式碼，目前主要的殭屍網路大多是由此延伸而來。

Kaiten :

亦稱為 Tsunami，可說是這三套基礎程式碼當中最鮮為人知的一套。Kaiten 是以暴力登入 Telnet 服務的方式散布，其最新的變種具備清除其他殭屍網路的功能，會將裝置上已經感染的其他殭屍網路清除。

Qbot:

雖然比 Kaiten 新一點，但也是個歷史久遠的 IoT 殭屍網路惡意程式，有許多稱號例如：Bashlite、Gafgyt、Lizkebab 或 Torlus。如同 Kaiten 一樣，Qbot 的變種也具備清除殭屍網路的功能，會將裝置上的其他殭屍網路惡意程式移除。

Mirai:

是三套基礎程式碼當中最普遍、也最廣為人知的一套。曾因癱瘓了各種大型網站和網路服務而聲名大噪。它一開始就被設計成一套專門用來販售的 DDoS 工具，並以遊戲玩家為攻擊目標。有些 Mirai 變種會清除裝置上已經感染的殭屍網路，好讓它能獨占裝置上的資源。

另外，由於 IoT 持續發展，使得殭屍網路有更大的發展空間，目前有五個 P2P IoT 殭屍網路惡意程式家族。

Wifatch :

最早出現於 2014 年的 Wifatch 是第一個具備 P2P 功能的 IoT 惡意程式。它被歸類為「羅賓漢」(Robin Hood) 惡意程式，因為其作者宣稱他設計這款程式的目的是為了保護路由器，用來防範其他那些真正的惡意程式。Wifatch 使用一種以 Perl 程式語言撰寫的客製化簡易 P2P 通訊協定。

Hajime :

Hajime 出現於 2016 年，它一開始常被拿來跟 Mirai 做比較，因為兩者所攻擊的目標裝置有許多重疊。但與 Mirai 不同的是，Hajime 不具備攻擊第三方機構的能力，但具備了 P2P 功能。Hajime 採用 DHT (Distributed Hash Table) 通訊協定，這也是 BitTorrent 分散式檔案系統的各節點之間同步時所用的通訊協定，因此不需中央伺服器。

Hide ‘n’ Seek :

Hide ‘n’ Seek (HNS) 在 2018 年現身，該年也是它的鼎盛時期。HNS 是利用漏洞來散播，其中有兩個是 IP 監視攝影機的漏洞。所以，HNS 很可能不光只攻擊路由器而已。我們在 2020 年 9 月研究 HNS 時發現它的活動量並不高，顯示其作者和營運者已經放棄該惡意程式。它值得注意的地方是採用了客製化 P2P 通訊協定來讓各節點從網路接收遠端指令。

Mozi:

最早出現於 2019 年的 Mozi 具備大多數現代 IoT 惡意程式的功能。它會用程式內有一份寫死的常見登入憑證清單以及某些漏洞來感染裝置。並採用 DHT 通訊協定來下載並驗證某個組態設定檔案。

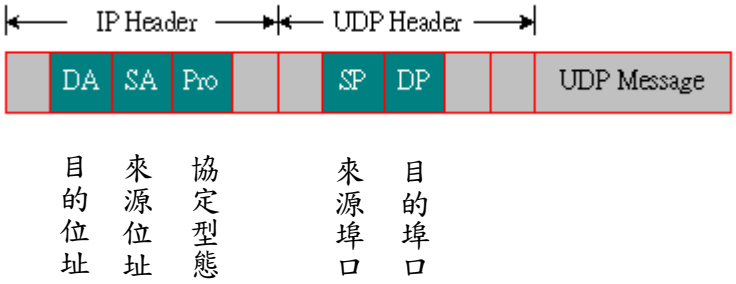
HEH:

HEH 最早出現於 2020 年，HEH 擁有現代化惡意程式的特質，是採用目前正夯的 Go 語言所開發。它會用程式內寫死的一份登入憑證清單與密碼來暴力登入裝置。值得注意的是，它會隨機掃描某些 IP 位址來尋找可感染的裝置，並利用演算法從 IP 位址計算出它所使用的 P2P 通訊埠編號。此殭屍網路顯然是專為賺錢而設計，具備攻擊第三方機構的潛力。

二、 防禦方法

一、 UDP 封包過濾

UDP 協定是屬於非連接方式，每一個封包都是獨立的，因此，決定 IP/UDP 封包是否給予通過的判斷訊息如下圖所示：



對於 UDP 攻擊來說，直接將封包擋住是最直觀的防禦方式，上方 UDP 的封包格式，可以觀察到有幾個欄位是可以操作的：

1. IP address
2. Port
3. UDP Message 長度

第一點 IP address，就是觀察 DA 欄位(SA 是自己)，基本上就是擋一些 IP 太奇怪的(像是 Local 的)，又或者是看看有沒有某個 IP 在短時間內發給你一堆封包，如果有就不要再接收他的封包。

第二點 Port(端口)，可以查詢自身的電腦應用程式有哪些是需要接收 UDP 封包的，其他的 Port 就丟掉。

第三點 UDP Message 長度，如果 UDP 攻擊送一些大封包給被害者主機，網路層會自動將大封包分段，我們可以將超過門檻而導致自動分段的封包都捨棄，達到防禦 UDP 的效果，但是需要小心過濾掉其他正常的封包，這樣會讓某些程式無法提供正常服務。

二、 限制 ICMP 數據包的 response rate

大多數 os 都會限制 ICMP 數據包的 response rate，部分原因是為了中斷需要 ICMP response rate 的 DDoS 攻擊。 這種緩解措施的缺點是，在攻擊過程中，合法數據包也可能在此過程中被過濾掉。 如果 UDP flood 的數量足以使目標服務器防火牆的狀態表飽和，則在服務器級別發生的任何緩解措施都將不足。

三、 使用 Anycast 技術

Anycast 是一種 network addressing 和 routing method。其中傳入的 request 可以 routing 到各種不同的位置或"nodes"。在 CDN 的上下文中，任播通常將傳入流量路由到最近的 data center，並具有高效處理請求的能力。選擇性 routing 允許 Anycast 傳播網絡在面對高流量、網絡擁塞和 DDoS 攻擊時具有彈性。

如果同時向某個 server 器發出許多請求，server 可能會被流量淹沒並且無法有效響應額外的傳入請求。使用 Anycast 播網絡，負載也可以分散到其他可用的 data center，而不是某個 server 首當其衝，每個數據中心都有能夠處理和回復傳入請求的服務器。這種路由方法可以防

止源服務器擴展容量，並避免對從源服務器請求內容的客戶端的服務中斷。

四、 使用雲端伺服(Azure 、CloudFlare) 之類的代理服務

對於較小的網站，您可以使用 CloudFlare 之類的代理服務。CloudFlare 通過控制域的 DNS 來工作。然後，它通過其網絡和服務器代理所有網絡流量，這些網絡和服務器經過高度強化以抵禦 DDoS 攻擊，並攔截其他常見的黑客嘗試，如 XSS 和 SQL 注入。然後將合法流量轉發到您的 Web 服務器，同時將可疑流量丟棄到上游，讓你不受潛在 DDoS 的影響。

三、 歷史案例探討

1. 前言

近年來有關 DDOS 的攻擊方式越來越多，每年都有新的工具或者是新的漏洞可以利用，而資安意識的抬頭造就了更多的防禦方法，也讓許多舊的攻擊方法被淘汰，接下來我們會探討有關 DDOS UDP Flood 的歷史案件，由此來研究 DDOS 的變遷。

2. 台灣學校攻擊事件

事件發生在 2012 年年末，是一起發生在台灣學術網的攻擊，因為有些學校公共電腦為了方便管理帳號密碼都很隨意，被攻擊者從遠端登陸主機，而後透過 IRC 伺服器發動攻擊。

3. Spamhaus 攻擊事件

Spamhaus 是一個處理電子郵件垃圾郵件的組織，事件發生在 2013 年年初，起因疑似是一場商業糾紛，攻擊者利用 Open DNS Server 的漏洞控制了許多主機，然後透過 DNS 的放大封包的機制，對 Spamhaus 發動攻擊，流量最高來到 300G bps 攻擊持續了一周。

4. 雲端主機攻擊事件

事件發生在 2020 年，攻擊 IP 超過十萬且 IP 位置分散，攻擊埠號為 6666 也是常用於 IRC 通訊，此次事件可能利用了木馬程式或是後門程式，組成了規模龐大的殭屍網路來攻擊，流量最高來到 1490G bps，攻擊持續了 5 分鐘。

5. 結語

經過時代變遷，可以看出以下變化：UDP 攻擊的流量逐年增加，小規模的 DDOS 次數也增加，這兩點都可以歸咎為電腦與網路的普及，電腦使用者越來越多網速也變得更快了。單純的 UDP 攻擊在大型攻擊上越發少見，因為大多數的組織都有對應 UDP 攻擊的經驗，而且因為資安意識的抬頭，長時間製造大量的殭屍網路也越來越困難。小規模的 UDP 攻擊大多是個體用戶的攻擊，UDP 的工具十分常見，甚至只需要幾個指令就可以製造出小規模的 UDP 攻擊，入門門檻低，所以 UDP 攻擊常常成為網路上私人怨恨的報復手段。

經過上方的探討，我認為未來 DDOS 的頻率以及規模都會繼續增大，大型攻擊將會是混合數種 DDOS 手段的混合式攻擊，而除了大型公司/組織需要提防 DDOS 攻擊之外，所有的電腦用戶都需要具備這方面的知識和意識，因為未來 DDOS 不再是大型組織的遊戲，過於方便的工具讓每個電腦用戶都可以隨時發動一場微型的 DDOS 攻擊。

四、 參考資料

1. 什麼是 IoT 殭屍網路？ [link]
2. 看清殭屍網路肆虐真相 [link]
3. 殭屍網路 [link]
4. Wiki [link]
5. TCP 三向握手 [link]
6. UDP flood attack [link]
7. DDos 攻擊介紹 [link]
8. 使用代理服務 [link]
9. Anycast 介紹 [link]
10. 其他參考資料

    甲、 臺灣學術網路危機處理中心團隊 [link]

    乙、 行政院國家資通安全會報技術服務中心 [link]

    丙、 威睿 DDoS 安全防禦團隊 [link]